

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 13-CR-120

PAUL D. CASE,

Defendant.

**UNITED STATES' RESPONSE TO DEFENDANT'S
MOTION TO SUPPRESS EVIDENCE**

The United States of America, by and through its attorneys, James L. Santelle, United States Attorney, and Benjamin W. Proctor, Assistant United States Attorney, hereby submits the following response to defendant Paul D. Case's "Amended Motion to Suppress" filed on November 7, 2013. (Doc. #22.)

In his motion, Case contends that the evidence seized during the search of his residence on May 2, 2013, as well as his statements to agents following the search, must be suppressed because of a defect in the search warrant affidavit. Specifically, Case contends that the affiant for the search warrant "intentionally omitted material facts." (Doc. #22 at 1.) In the hopes of producing some support for this bold assertion, Case requests an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978).

For the reasons discussed in detail below, Case has wholly failed to make the required "substantial preliminary showing" necessary for the Court to hold *Franks* hearing. As such, the motion must be denied.

I. BACKGROUND

This case began through an online investigation into the sharing of child pornography through the Ares peer-to-peer network. (*See* Response Exhibit B (“Ex. B”) ¶25.) On April 24, 2013, FBI Task Force Officer Brant Ungerer obtained a search warrant to search Paul Case’s residence. (*See* Ex. A.) In support of the search warrant, TFO Ungerer submitted a 19-page affidavit setting forth the basis for probable cause to believe that the target residence concealed evidence relating to the distribution and possession of child pornography. (*See* Ex. B.)

The affidavit noted that the information was based on TFO Ungerer’s investigation as well as information provided to him by other law enforcement personnel. (Ex. B. ¶3.) It further noted that the information is submitted for the limited purpose of securing a search warrant and does not set forth every fact related to the investigation. (Ex. B ¶3.)

The affidavit sets forth the facts relevant to the investigation. It addresses, among other things, the role played by internet service providers (ISPs), identifiers used in software applications, the nature of peer-to-peer networks and specifically the Ares peer-to-peer network, how files are identified and shared through the internet using peer-to-peer programs, and how files and remnants of files are stored on computers. (Ex. B ¶¶7-13.)

The affidavit goes on to discuss the results of this particular investigation. For purposes of this motion, the following paragraphs of the search warrant affidavit are particularly relevant:

25. On November 24, 2012, around 2:11 a.m. Central Standard Time (“CST”), Online Covert Employee 5023 (“OCE-5023”), acting in an undercover capacity, conducted investigations into the sharing of child pornography files on the Ares P2P file sharing network. During this time, OCE-5023 identified a computer with the IP address 174.102.233.53 with at least seven files of investigative interest available for download.

26. During the investigation, the Ares client P2P program on the computer with the IP address 174.102.233.53 reported its version as 2.1.8.3042, and its ARES nickname as: anon_ae66e935@Ares. Of note, this P2P file sharing program has been enhanced to ensure that downloads occur only from a single selected source.
27. Between 02:11 a.m. CST on November 24, 2012, and 03:33 a.m. CST on November 25, 2012, OCE-5023 successfully completed downloads of five files containing child pornography from the computer at IP address 174.102.233.53, including the following three files:

(Ex. B ¶¶25-27.) The affidavit goes on to provide the file names, hash values, and descriptions of the three files. It then discusses how agents were able to tie IP address 174.102.233.53 to the defendant, Paul Case. (Ex. B ¶¶28-34.) The affidavit further describes the place to be searched (Case's residence) and the items to be searched or seized (computers and related items). (Ex. B ¶¶39-40.)

FBI Task Force agents executed the search warrant at Case's residence on May 2, 2013. At that time, agents recovered several computers from the residence, as well as other items. Following the search, Case was read his rights and agreed to answer questions from agents. Case eventually admitted to agents that he used one of the computers recovered from the residence, a Dell laptop, to view child pornography for several months prior to the execution of the search warrant. He admitted that about a month before the search, he decided to stop viewing the child pornography and conducted a "factory reset" on the computer. He further admitted that he knew the Ares peer-to-peer program was installed on the computer and that he was familiar with how peer-to-peer file sharing programs operate. He admitted that he knew the "shared" folder for the Ares peer-to-peer program contained child pornography files and that it was sharing these files through the internet. A forensic examination of the Dell laptop turned up several videos of child

pornography in unallocated space as well as evidence of the child pornography files downloaded by agents during the online investigation of November 24-25, 2013.¹

On July 2, 2013, a grand jury in this District returned an indictment charging Paul Case with two counts: (1) distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2); and (2) possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). (Doc. #1.) An arraignment was held on July 8, 2013. Thereafter the Court granted two motions filed by Case seeking additional time to file pretrial motions. (Docs. #11, 15.) A superseding indictment was filed on November 5, 2013, which amended the date associated with Count Two. (Doc. #19.) On November 6, 2013, Case filed the instant motion. (Doc. #21.) An amended version of motion was filed on November 7, 2013. (Doc. #22.)

III. ARGUMENT

Case seeks to suppress physical evidence seized by agents during the search of May 2, 2013, along with his statements to agents following the search, under the doctrine set forth in *Franks v. Delaware*, 438 U.S. 154 (1978). Specifically, he asserts that “the [search] warrant was based on an affidavit that intentionally omitted material facts.” (Doc. #22 at 1.) He therefore requests a *Franks* hearing “to show that agents made material omissions in the affidavit in support of the warrant that were in reckless disregard of the truth.” (Doc. #22 at 4.)

In order for Case to be entitled to a *Franks* hearing, he “must make a ‘substantial preliminary showing’ that: (1) the affidavit contained a material false statement; (2) the affiant made the false statement intentionally, or with reckless disregard for the truth; and (3) the false statement was necessary to support the finding of probable cause.” *See United States v. Maro*, 272 F.3d 817, 821 (7th Cir. 2001) (quoting *Franks*, 438 U.S. at 155-56). Allegations that the

¹ These facts are pulled from reports produced by law enforcement during the investigation. All of these reports have been turned over to the defense in discovery.

affidavit omitted material statements are subject to the same standard. *See United States v. Williams*, 737 F.2d 594, 604 (7th Cir. 1984).

The burden on the movant in seeking a *Franks* hearing is “substantial.” *United States v. Johnson*, 580 F.3d 666, 670 (7th Cir. 2009). “[A]ffidavits supporting a search warrant are presumed valid, and . . . the ‘substantial preliminary showing’ that must be made to entitle the defendant to an evidentiary hearing must focus on the state of mind of the warrant affiant, that is the police officer who sought the search warrant.” *United States v. Jones*, 208 F.3d 603, 607 (7th Cir. 2000) (citing *Franks*, 438 U.S. at 171). “The defendant must offer evidence showing either that the warrant affiant lied or that the warrant affiant recklessly disregarded the truth because he ‘in fact entertained serious doubts as to the truth of his allegations’ or had ‘obvious reasons to doubt the veracity of the allegations.’” *Id.* (citing *Williams*, 737 F.2d at 602); *see also generally United States v. Bershchansky*, Case No. 12-CR-00064, 2013 WL 3816570 (E.D.N.Y. July 19, 2013) (denying request for *Franks* hearing in challenge to child pornography search warrant affidavit, noting “[t]o avoid ‘fishing expeditions into affidavits that are otherwise presumed truthful . . . [the defendant] should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons.’” (quoting *United States v. Falso*, 544 F.3d 110, 125-126 (2d Cir. 2008)). Negligence by the affiant does not constitute reckless disregard for the truth. *See United States v. A Residence Located at 218 Third Street*, 805 F.2d 256, 258 (7th Cir. 1986). With this in mind, “*Franks* hearings are rarely required.” *Johnson*, 580 F.3d at 670 (citing *Maro*, 272 F.3d at 821);

A. Case Fails to Make a “Substantial Preliminary Showing” that the Search Warrant Affidavit Included a False Statement or Omitted a Material Fact.

In his motion, Case asserts that the search warrant affidavit is misleading because “agents did not personally observe the facts recited in the affidavit, but instead utilized a secret and classified automated version of the ‘RoundUp Ares’ program to secure all other information than that obtained by the subpoena to the Internet Service Provider (ISP) for the physical address where the computer was located.” (Doc. #22 at 1-2.)² In support of this conclusory assertion, Case states that “Agent K. Kolecheck admitted to Case’s computer forensic expert that RoundUp program ran unattended during the time which encompasses Count One of the Indictment.” (Doc. #22 at 2.) The motion continues: “Thus application in support of the search warrant is misleading in its use of the words sessions and investigation. A. The sessions are automated, unattended, and logged. B. The investigation is done by the program, not a person.” (Doc. #22 at 2.)

There are several fatal problems with Case’s allegations. First, the underlying (and hearsay) assertion is simply wrong. FBI ITS Forensic Examiner Kerry Kolecheck did not tell Case’s computer forensic expert that “RoundUp ran unattended” during the investigation that led to charges against Case. (*See* Ex. C.) And in any event, the search warrant affidavit, sworn to by

² In his motion, Case separates his allegations into 15 numbered paragraphs that purport to relate to the investigation in this matter. (Doc. #22.) However, he does not articulate which of these assertions were required to be included in the affidavit in order to save the affidavit from being misleading. Paragraphs 1, 5, 7, 11, 12, and 15 appear to be mostly arguments and opinion. And, as discussed herein, it is unclear how the omission of any allegations of “fact” included in paragraphs 2, 3, 4, 6, 8, 9, 10, 13 and 14 are material to the finding of probable cause. The only support Case provides for the allegations included in his motion is an affidavit based on information and belief submitted by his counsel. (Doc. #22-1.) However, this document in turn includes a mix of opinions, arguments, and allegations of fact. The United States takes issue with many of the arguments and assertions in Case’s motion and affidavit. Many of them are simply wrong and/or irrelevant. But, because Case’s burden at this stage is to put forward a “substantial preliminary showing,” the United States has focused its response on the elements relevant to the *Franks* inquiry as directed by controlling law.

TFO Ungerer, specifically notes the active involvement of agents in the investigation. (*See e.g.*, Ex. B ¶¶25-27.)

Second, the affidavit does not appear to include the word “sessions.” Hence, Case’s assertion that the “application in support of the search warrant is misleading in its use of the word[] session” can be dismissed.

Third, it is unclear what Case means in stating that the use of the word “investigations” rendered the affidavit misleading because it involved a computer program.³ Is he contending that the affidavit gives the impression that agents did not use a computer program in this investigation regarding online sharing of child pornography on the Ares peer-to-peer network? This would make little sense. Indeed, law enforcement investigations into the online sharing of child pornography via peer-to-peer networks are nothing new.⁴ Moreover, the affidavit in this case includes several paragraphs describing the nature of peer-to-peer file sharing and other background information, and Paragraph 25 specifically states that case agents “conducted investigations into the sharing of child pornography files on the Ares P2P file sharing network. During this time, [case agents] identified a computer with the IP address 174.102.233.53 with at least seven files of investigative interest available for download.” (Ex. B ¶25) The affidavit goes on to state that the Ares program used in the investigation “was enhanced to ensure that

³ The word “investigation” appears 14 times in the affidavit in varying contexts.

⁴ *See e.g.*, *United States v. Annoreno*, 713 F.3d 352, 355 (7th Cir. 2013) (addressing sentencing challenge, and noting “[i]n peer-to-peer file sharing, users make specific files and videos containing child pornography available to others in exchange for access to such files on other users’ computers.”); *United States v. Klug*, 670 F.3d 797, 798 (7th Cir. 2012) (“Klug came to the attention of law enforcement after an FBI agent, using a peer-to-peer network, discovered that an Internet address assigned to Klug was being used to share child pornography.”); *United States v. Carani*, 492 F.3d 867, 876 (7th Cir. 2007) (discussing peer-to-peer file sharing and noting that distribution enhancement under U.S.S.G. § 2G2.2(b)(3)(B) was appropriate for child pornography prosecution where defendant “made his child pornography videos available through [peer-to-peer file sharing program] Kazaa”).

downloads occur only from a single selected source”⁵; that agents identified and successfully downloaded several suspected child pornography files; the dates the downloads were performed; and the contents of the downloaded files. (Ex. B. ¶¶25-27.)

Case also states that there is a “high likelihood that RoundUp software anonymously invades parts of the target computer other than the file sharing program.” (Doc. #22 at 4.) But he does not provide any support for this bold assertion. Moreover, this assertion conflicts with the statements in the search warrant affidavit, which states that this investigation concerned child pornography files being shared through the Ares peer-to-peer file sharing program. Among other things, the affidavit goes into detail noting the version of Ares being run on Case’s computer, the files Case’s computer had available for download, and the Ares nickname used by Case’s computer. (See, e.g., Ex. B ¶¶7-12, 25-27.) And, evidence of this Ares peer-to-peer program, as well as evidence of files matching those identified and downloaded by agents during the November 2012 investigation, were found on Case’s computer after the search. If Case is trying to imply that statements in the affidavit regarding the nature and conduct of the investigation are somehow false, then he was required to present supporting evidence for such a charged claim in this motion.⁶ As noted above, the affidavit is presumed to be valid, and the Seventh Circuit has repeatedly stated that “[c]onclusory, self-serving statements are not enough to obtain a *Franks* hearing.” *Johnson*, 580 F.3d at 671 (citing *Franks*, 438 U.S. at 171); see, e.g., *United States v. Reed*, 726 F.2d 339, 342 (7th Cir. 1984) (“[T]he *Franks* presumption of validity of an affidavit supporting a search warrant cannot be overcome by a self-serving statement which purports to

⁵ This is relevant as Paragraphs 11 and 12 of the search warrant affidavit discuss the nature of the Ares network and the occurrence of “multiple source downloads.” (See Ex. B ¶¶11-12.)

⁶ Of note, Case has been provided in discovery with the logs and records of the undercover operation of November 24-25, 2013, as well as the forensic examination report of Case’s computer. These logs, records, and examination reports support the assertions in the search warrant affidavit.

refute the affidavit.” (citation omitted); *see also e.g., United States v. Collins*, 753 F. Supp. 2d 804, 811-12 (S.D. Iowa 2009) (noting inter alia that defendant’s general assertions regarding law enforcement peer-to-peer investigative software were not sufficient to meet “substantial” burden required to obtain *Franks* hearing); *United States v. Hibble*, Case No. CR 05-1410, 2006 WL 2620349 (D. Ariz. Sept. 11, 2006) (denying defendant’s request for *Franks* hearing based on alleged omissions in search warrant affidavit that discussed online investigation into sharing of child pornography on peer-to-peer network).

B. Case Fails to Make a Substantial Preliminary Showing that the Inclusion of the Allegedly Omitted Facts in the Affidavit Would Negate a Finding of Probable Cause.

Perhaps most importantly, Case fails to explain how any of the allegations in his motion are *material* to the finding of probable cause. An omitted fact is not material unless its inclusion would prevent the affidavit from supporting a finding of probable cause. *See Williams*, 737 F.2d at 604; *see generally Maro*, 272 F.3d at 821 (7th Cir. 2001) (noting that unimportant allegations, even if untrue or misleading, are not sufficient to trigger the need for a *Franks* hearing).

Here, the search warrant affidavit supports a finding of probable cause that Paul Case’s residence concealed evidence of violations of 18 U.S.C. § 2252A. Case’s burden in seeking a *Franks* hearing is to make a “substantial preliminary showing” that the inclusion of the allegedly omitted fact(s) would destroy such a finding.

Case is unable to meet this burden. Nothing in Case’s motion calls into question key facts supporting probable cause, including: (1) agents conducted an investigation into the online sharing of child pornography through the Ares peer-to-peer network; (2) agents identified several files of suspected child pornography on a computer running Ares peer-to-peer program with IP

address 174.102.233.53; (3) agents successfully downloaded several illegal files from this computer; and (4) agents determined that Paul Case was the subscriber associated with that computer and IP address. Under these circumstances, a *Franks* hearing would serve no purpose. *See United States v. Carmel*, 548 F.3d 571, 577 (7th Cir. 2008) (“[I]f probable cause to issue the warrant would still exist even if the false statement or material omission were corrected, then no *Franks* hearing is required. “ (citing *United States v. Souffront*, 338 F.3d 809, 822 (7th Cir. 2003)).⁷

C. Case Fails to Make a Substantial Preliminary Showing that the Affiant Intentionally or Recklessly Omitted Facts from the Affidavit.

Finally, Case fails to address the requirement that he make a “substantial preliminary showing” that a material omission (whatever it may be) was made intentionally or with reckless disregard for the truth. In order to obtain a *Franks* hearing, Case’s burden is to ““offer direct evidence of the affiant's state of mind or inferential evidence that the affiant had obvious reasons for omitting facts in order to prove deliberate falsehood or reckless disregard.”” *Souffront*, 338 F.3d at 822 (7th Cir. 2003) (citing *United States v. McNeese*, 901 F.2d 585, 594 (7th Cir. 1990), *overruled on other grounds as recognized by United States v. Westmoreland*, 240 F.3d 618, 632–33 (7th Cir. 2001)).

Here, Case provides no showing of falsity on the part of the affiant. While the many unsupported and conclusory allegations in the motion seem to point fault at the “law enforcement” in general, there is nothing to indicate that the affiant in this case lied or otherwise recklessly disregarded the truth in his affidavit. As Case concedes, he has no evidence on this

⁷ Case mentions in his motion that “the good faith doctrine does not save this search because law enforcement officers engaged in *parallel construction*.” (Doc. #22 at 1.) Case provides no support for this assertion. Moreover, before a discussion of the good faith exception, as discussed in *United States v. Leon*, 468 U.S. 897, 914, 923 (1984) and related cases, is appropriate, Case would first need to establish that the alleged omissions were material to the finding of probable cause. For the reasons discussed, he has not done so.

point; the reason he requests a *Franks* hearing is to try to fish for evidence. (See Doc. #22 at 4 “Case requests a hearing to show that agents made material omissions in the affidavit in support of the warrant that were in reckless disregard of the truth.”). Such an approach conflicts with the limited purpose of a *Franks* hearing. See *Franks* 438 U.S. at 171; *United States v. McAllister*, 18 F.3d 1412, 1416 (7th Cir. 1994) (“[A]s the *Franks* Court went on to explain, to mandate an evidentiary hearing for the purpose of challenging a warrant affidavit, ‘the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine’ the affiant.” (quoting *United States v. Radtke*, 799 F.2d 298, 310 (7th Cir. 1986))). As Case is unable to support his assertions, the motion can be denied.

III. CONCLUSION

This case is not complicated. Agents conducted an online investigation into the sharing of child pornography over a public file-sharing network. Though this investigation, agents located and downloaded child pornography files from a computer using an IP address that was indisputably tied by Paul Case. With this information, the case agent sought and obtained a warrant to search Paul Case’s house for evidence of child pornography.

Case’s motion seeks suppression under *Franks v. Delaware*. The focus is on the veracity of the search warrant affidavit and the conduct of the affiant. Therefore, the law requires at the outset that Case make a “*substantial preliminary showing*” that an evidentiary hearing will expose the search warrant affidavit as intentionally or recklessly false. He has not, and cannot, do so. In fact, it is apparent from the content of the motion that Case seeks a *Franks* hearing in order to try to substantiate his speculative assertions. Such an approach is never warranted, and

for the reasons set forth above, the United States respectfully requests that the Court deny Case's request for a *Franks* hearing and deny Case's motion to suppress evidence.

Dated at Milwaukee, Wisconsin, this 18th day of November, 2013.

Respectfully submitted,

JAMES L. SANTELLE
United States Attorney

By: s/ Benjamin W. Proctor

BENJAMIN W. PROCTOR
Assistant United States Attorney
Benjamin Proctor Bar No.: 1051904
Attorney for Plaintiff
Office of the United States Attorney
Eastern District of Wisconsin
517 E. Wisconsin Ave. Suite 530
Milwaukee, Wisconsin 53202
Tel: (414) 297-1700
Fax: (414) 297-1738
Email: benjamin.proctor@usdoj.gov